LES DOSSIERS TECHNIQUES

GERER LA SECURITE D'UN SITE DE COMMERCE ELECTRONIQUE

Mai 2001

Version 1.0

Commission Réseaux et Systèmes Ouverts

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, Rue Pierre Sémard – 75009 Paris
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document :

Laurence	**Berranger**	Thomson CSF Detexis
Alain	**Bourges**	Ministère de la Défense
Philippe	**Conversin**	6Wind
Paul	**Constant**	Paul Constant Conseil
Michèle	**Copitet**	Egona Consulting
Jean-François	**Fava-verde**	Racal Security & Payments
Jean-François	**Gonel**	AFP
Jacques	**Gonik**	
Paul	**Grassart**	CLUSIF
Rachid	**Mesbahi**	FNMF
Lazaro	**Pejsachowicz**	Bull
Stéphane	**Plichon**	Gemplus
Paul	**Richy**	France Télécom
Jean-Louis	**Roule**	Jean-Louis Roule Conseil
Hervé	**Schauer**	HSC

Table des matières

1 Introduction

1.1 Positionnement du problème

L'impact d'Internet sur notre façon de penser et d'agir à un effet irréfragable, tant sur les plans humains, techniques, économiques, qu'organisationnels. Nos habitudes s'en trouvent quelque peu bousculées, voire transformées, car ce concept de communication, relativement nouveau, influe de façon significative sur les règles du jeu et en particulier sur celles de la compétition. Ce changement imprévisible a, entre autres, crée une situation d'incertitude mettant en cause notre cadre intellectuel et notre mode de pensée. Cette incertitude est probablement liée à la non maîtrise de la rapidité d'évolution des comportements et au modèle économique qui va structurer cette nouvelle forme de distribution.

Le commerce, dans son sens général, n'échappe pas à cette transformation. Pour positionner le problème, nous considérerons dans cette étude que **le commerce électronique est l'ensemble des échanges numérisés liés à des activités commerciales : entre entreprises, entre entreprises et particuliers ou entre entreprises et administrations.**

Les moyens employés pour ces échanges ne sont pas nouveaux, mais sont divers, puisqu'ils vont du téléphone à la télévision numérique en passant par les liaisons informatiques spécialisées ou le Minitel… Les échanges de données informatisés (EDI) se sont largement développés au cours des dix dernières années, entre entreprises et entre entreprises et administrations.

L'émergence accélérée d'Internet modifie considérablement ce contexte, car son coût réduit et sa relative simplicité d'utilisation favorisent une diffusion très rapide, notamment vers les petites entreprises et vers les consommateurs.

Ces technologies en progrès rapide peuvent constituer une opportunité majeure pour les entreprises et les consommateurs. Si le développement de la vente électronique des produits et services constitue aujourd'hui le phénomène le plus médiatisé, il n'en est pas pour autant le seul.

Un des éléments non négligeables qui caractérise aussi ces systèmes, est que la « banque électronique » fait partie de cet ensemble. Par ailleurs les entreprises ont à repenser profondément leurs modes de fonctionnement en les structurant autour des flux d'informations.

Cette nouvelle dynamique de marché, caractérisée par la dématérialisation des transactions et leur indépendance par rapport à la géographie et aux frontières, remet en cause la pertinence et l'efficacité des règles et obligations définies par les états et organisations internationales. De nouvelles règles du jeu s'esquissent et la préservation des valeurs communes aux pays

européens doit être prise en compte vis-à-vis de l'avance que peuvent avoir les Etats-Unis en la matière.

Pour permettre aux entreprises et aux consommateurs de tirer le meilleur parti des opportunités nouvelles, le cadre législatif et réglementaire doit évoluer rapidement pour accroître la **« confiance »**. L'avenir du commerce électronique dépend aussi de la croissance du nombre d'utilisateurs d'Internet, qu'ils soient vendeurs ou d'acheteurs.

Cette magnifique médaille a son revers, car cette approche qui favorise le développement d'activités nouvelles et innovantes et qui donne aux différents acteurs des chances de « gagner », peut, du fait des **vulnérabilités** qu'elle introduit via ses systèmes et les technologies utilisées, les conduire au risque de tout perdre.

La « mauvaise qualité » de certains sites de commerce électronique, sur le plan de leur développement (conception et réalisation) et la « porosité » que présentent de nombreux systèmes sur lesquels ils s'appuient, contribuent au manque de confiance que peut susciter cette évolution.

Par sa vocation sécuritaire le CLUSIF peut apporter, en diffusant des préconisations sur ce sujet, une contribution significative dans la qualité des solutions à retenir pour résoudre les divers problèmes liés à leur sécurité.

1.2 Objet de ce document

Ce document à pour objet :

- De produire une ensemble de préconisations, de consignes, voire de recommandations dans la démarche à suivre et dans les solutions de sécurité à retenir pour mettre en œuvre et exploiter les systèmes propres au Commerce Électronique.
- De donner une classification des sites de Commerce Électronique selon leur spécificité.
- De recenser les différentes natures de menaces qui pèsent sur ces systèmes et de préciser les risques qu'elles peuvent faire naître.
- De proposer dans les principaux domaines de sécurité, sur les plans physiques, logiques et organisationnels, les différents services, mécanismes… moyens de sécurité classiques qui relèvent de la sécurité d'une infrastructure réseau et qui entrent dans les solutions de sécurité à mettre en œuvre.
- De préciser les droits, devoirs et responsabilités des principaux acteurs ou partenaires impliqués dans la conception, l'exploitation et l'utilisation de ces systèmes.

Ce documents est destinés à l'ensemble des membres du CLUSIF :

- aux RSSI dans le cadre de leur mission de conseil auprès :
  - des concepteurs et développeurs du projet de Commerce Électronique,
  - des opérateurs chargés de l'exploitation du site.
- Aux Offreurs qui interviennent par leurs prestations dans le cadre de développement de tels Systèmes.

2 Les acteurs du commerce électronique

Le commerce électronique ne peut pas être analysé simplement comme un ensemble de « programmes d'ordinateur » mis en relation.

Un nombre important d'acteurs, personnes, fonctions ou institutions interviennent dans un système de commerce électronique, avec des besoins (et donc des perceptions des menaces) différents.

Une vision très globale nous donne trois types d'acteurs ayant des points de vue bien différents : les clients, les vendeurs et les intermédiaires techniques. Mais, dans la pratique, un quatrième type d'acteur se dégage, essentiel pour le bon déroulement des transactions commerciales, l'intermédiation financière simple ou multiple, faisant office parfois de lien de confiance entre les clients et les vendeurs/fournisseurs.

Bien sûr, une vision détaillée nous permettra de voir que ces trois grands types d'acteurs, peuvent être décomposés de façon à permettre une analyse plus fine des menaces principales les concernant dans le cadre du commerce électronique.

Pour la bonne compréhension de ce document, rappelons que la dénomination « Commerce Électronique » couvre aujourd'hui des services plus ou moins complets du Web allant de la simple présentation du catalogue jusqu'a des transactions de vente, paiement et livraison de marchandise.

Le schéma suivant montre une structure classique d'hébergement d'un site marchand et positionne les acteurs.

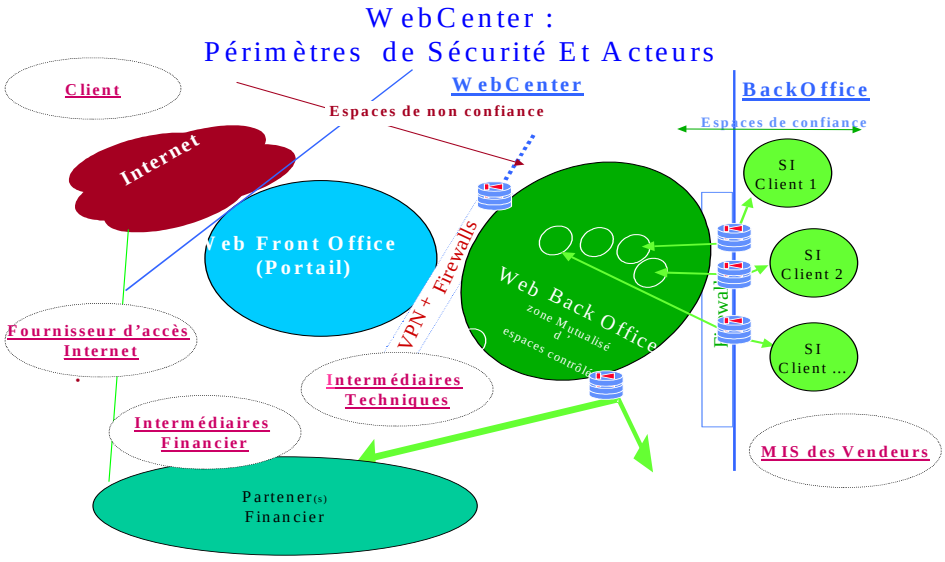

Figure 1 : structure classique d'hébergement d'un site marchand et positionnement des différents acteurs

2.1 Le Client

Le client est bien sur, l'élément central d'un système de commerce électronique. Il est donc l'objet de toutes les attentions mais aussi de toutes las convoitises. Il est aussi en tant que personne l'objet d'une vaste législation en France qui, en protégeant le client, permet à celui-ci d'aborder avec confiance les nouveaux modes de commerce.

Le premier préalable d'un site de commerce électronique doit être donc le strict respect de cette législation . Bien que nous ne puissions pas aborder en détail cette législation ni au niveau Français ni au niveau international, deux cadres réglementaires s'appliquent aux sites de commerce électronique :

- celui qui découle du caractère de « commerce » (électronique ou pas) et qui est principalement concerné par les règles de la vente par correspondance (VPC), puisque c'est à celle-ci que la loi Française assimile le « commerce électronique ». Le droit du consommateur est, bien sûr, directement applicable à ces sites ;
- celui qui découle du caractère « électronique » des sites et que concernent principalement la protection des informations personnelles du client (Loi Informatique et Liberté) et l'application des lois concernant les publications (un Web est un moyen de publication qui doit être enregistré en tant que tel).

Ajoutons finalement qu'apparaissent dans le domaine de sites de commerce électronique des « labels » de certification, ayant pour objectif de garantir aux clients du site le respect de règles déontologiques, dont celles énoncées précédemment.

2.1.1 Le client individuel /occasionnel (particulier ou entreprise)

Il se « promène » sur le Web et accède aux sites de commerce électronique pour s'informer et/ou pour acheter.

À ce titre, il a besoin de savoir qu'il est sur le « bon » serveur, qu'il voit le « bon » produit, avec son « vrai prix ». Il peut donc craindre :

- la « mascarade » du serveur Web du site ;
- les atteintes à l'intégrité des informations du site.

De plus, il peut être sollicité par le site pour fournir des informations personnelles et/ou servant au paiement de la transaction. Il est donc concerné par la perte de confidentialité des informations personnelles et/ou financières.

2.1.2 Le client individuel identifié

Il subit les mêmes menaces que le précédent, mais les moyens de prévention sont plus faciles à mettre en œuvre. Par exemple, il est possible d'utiliser des méthodes de reconnaissance réciproque basés sur des connaissances mutuelles.

Par ailleurs, une fois identifié, le client peut supposer que des informations personnelles ou financières n'ont plus besoin d'être demandées.

Bien sûr, le simple mot « client identifié » nous met en face d'une problématique majeur du commerce électronique : quel méthode utiliser pour identifier un client (individuel ou entreprise)et quel confiance avoir dans cette identification.

Des méthodes et des outils ont bien était développés, notamment les Infrastructures à clé publiques (PKI), mais cet modèle, basé sur des certificats basés sur la technologie de chiffrement à clés publiques et des Autorités de Certification (voir document « Chiffrement » de notre commission), est trop lourd à mettre en œuvre à cause principalement des besoins de vérification on-line des certificats et autorités émettrices pour les différents certificats.

Mais des nouveaux approches apparaissent pour permettre une mise en œuvre des technologies solides, basés sur les mêmes concepts mais qui facilitent les tâches des acteurs devant s'identifier réciproquement.

C'est le cas du modèle « Four Corners » défini par le groupement Identrus, qui sera abordé dans le paragraphe relatif aux acteurs financiers.

2.1.3 Le partenaire

On peut le considérer comme un cas particulier de « client identifié », mais avec un volume de transactions bien plus élevé. Dans beaucoup de cas, les relations avec ces « partenaires » existent dans l'entreprise qui met en place le « Système de Commerce Électronique. »

Elles étaient et sont très fréquemment mises en œuvre par un système d'Échange Électronique des Documents (EDI). Nous ne traiterons pas ici ce type d'échange, le CLUSIF ayant déjà publié une méthode très complète pour l'analyse de ce type de relations, la méthode MESSEDI, que nous vous invitons à consulter.

Signalons pourtant que ce « partenaire », qui est fréquemment aussi revendeur, OEM ou ISV, utilisera de plus en plus le catalogue du vendeur affiché sur le site Web et sera donc de plus en plus concerné par la mascarade du serveur Web du site et les atteintes à l'intégrité des informations.

2.2 Le Vendeur

2.2.1 Le Vendeur Unique

Il s'agit d'une entreprise qui gère directement la commercialisation de son produit à travers un site Web qu'elle a mis en place. Dans ce cas, elle devra faire face à l'ensemble des menaces qui seront listées pour les types suivants, qui sont, pour la plupart le produit du découpage des fonctions de ce vendeur unique.

Il sera donc concerné par :

- les atteintes à la disponibilité de son/ses sites, produisant des pertes de vente et de clientèle ;
- une substitution de son site par des sites pirates produisant soit des pertes directes (ventes) ou indirectes (image de marque) ;
- des pertes d'intégrité du contenu de son site tel que les modifications des rubriques ou des prix du catalogue atteignant aussi bien des aspects légaux (responsabilité civile) que commerciaux (perte de ventes, image de marque, respect du prix catalogue) ;
- des mascarades, modifications ou répudiations de transactions, avant ou après livraison de la marchandise ;
- le non-paiement ou non-recouvrement des marchandises livrées.

2.2.2 Le Fournisseur de Catalogue à Vendeurs Multiples ou Portail Commercial

C'est dans les fait un cas très répandu aujourd'hui. Beaucoup d'enseignes, même si elles correspondent à des magasins « physiquement existants », se comportent sur le Web comme de simples intermédiaires vis à vis de leurs fournisseurs. C'est un cas très répandu dans le domaine de la vente des livres ou disques. Leur valeur ajoutée vient donc surtout du prestige de leur site, et ils sont donc concernés en premier lieu par la disponibilité du site et les menaces sur leur image de marque.

Cet acte d'intermédiation ne les dégage pas des obligations légales concernant leur responsabilité civile, le respect du prix catalogue et donc du devoir de se protéger contre les atteintes à l'intégrité du contenu du site. Cette même préoccupation d'intégrité de l'information doit guider tous les contrôles de transmission du catalogue entre les vendeurs finaux et le site « multi-catalogue ».

Par contre, les aspects financiers sont parfois gérés directement entre les intermédiaires financiers et les vendeurs finaux, le site Web se limitant à donner accès aux mécanismes de paiement.

2.2.2.1 Les Fournisseurs du Vendeur

Ils ne sont pas directement pris en compte dans cet ouvrage, sauf s'ils sont directement concernés par la transaction de vente (Voir « Fournisseurs de Catalogue…. »).

La prise en compte des relations entre une entreprise faisant du « Commerce Électronique » et ses fournisseurs par des moyens informatiques, correspond à un concept plus large couvert par l'anglicisme « e-Business », et que nous n'aborderons pas dans cet ouvrage.

Mais le lecteur pourra trouver beaucoup d'informations utiles concernant ces problèmes dans d'autres brochures du CLUSIF tels que les Méthodes Méhari et Messedi et, plus proche de la technique, Sécurité des pare-feu et Sécurité Intranet.

2.2.2.2 Les différentes fonctions internes du « Vendeur » (Marketing, Service Clients, Logistique…)

Les différents aspects du commerce électronique sont distribués parmi les différentes fonctions de l'entreprise bien que parfois, un départ « commerce électronique » joue le rôle du coordinateur de ces différents départements. Ainsi, le « marketing » sera plus directement concerné par les aspects intégrité du catalogue, la « logistique » par l'intégrité et la non répudiation des transactions et les « finances » par le recouvrement.

Une attention particulière doit être prêtée au Service Client. De plus en plus les entreprises mettent en œuvre des systèmes de suivi de la clientèle très élaborés, intégrant les informations reçues par le Web, non seulement pour la maintenance des produits achetés mais aussi pour développer une vraie politique de fidélisation de la clientèle, ce qui implique autant l'après-vente que le marketing.

Ces systèmes, appelés couramment CRM (Customer Relationship Management), couplés au site du "Commerce Électronique », sont extrêmement sensibles à l'intégrité des informations concernant les clients. En effet, les fausses informations à ce niveau seront autant de facteurs d'inefficacité des futures actions commerciales.

2.3 Les intermédiaires techniques

2.3.1 Le Fournisseur du Site de Commerce Électronique

Sa responsabilité s 'arrête théoriquement à la publication des informations du vendeur et à l'enregistrement et transmission des transactions. La disponibilité du site, et l'intégrité des informations transmises par le client.

Mais il est aussi co-responsable avec les fournisseurs d'information de la plupart des actes où la responsabilité civile de ce dernier peut être mise en cause, ainsi que de la protection des informations personnelles gérées par le site.

En fait, cette prestation globale est le plus souvent remplie par plusieurs fournisseurs différents dont la Maîtrise d'œuvre peut être réalisée parfois par le vendeur lui-même.

Nous détaillerons à continuation ces prestataires.

2.3.2 Le Fournisseur d'Accès Internet (« Internet Service Provider » ou ISP).

En principe, sa responsabilité se limite à la fourniture du « tuyau » de liaison avec Internet et des éléments nécessaires à son utilisation (adresses, serveur des noms, etc.).

Du point de vue de la sécurité il ne serait donc responsable que de la disponibilité de son « tuyau». Dans les faits, les ISP, outre le besoin d'offrir les meilleurs types de liaison vers le monde Internet, offrent de plus en plus de services et mécanismes de protection comme le filtrage des services non désirés, la protection contre certains types d'attaques et l'aide à l'enquête après incident.

2.3.3 L'exploitation des machines et l'administration des systèmes du site Web.

Cette tâche, qui est parfois cumulé avec la précédente, fournit la configuration des systèmes d'exploitation, l'installation des applications et du serveur Web et sa gestion récurrente.

Elle doit fournir tous les mécanismes de sécurisation du système et de configuration sécurisée du Web, complémentaires de ceux de l'ISP. En particulier, elle doit assurer la traçabilité des interactions et le filtrage des services si ces services ne sont pas assurés par l'ISP.

Plusieurs publications de notre commission (Sécurité Unix, Sécurité NT, Pare-feux, Sécurité Intranet) peuvent aider pour cette tâche.

2.3.4 Le concepteur et le gestionnaire du site Web.

Ces deux tâches sont bien souvent réunies.

C'est l'intermédiation technique entre les besoins de l'entreprise et les moyens techniques devant être mis en œuvre sur Internet.

Bien que l'essentiel du contenu doive recevoir l'accord du vendeur, il est responsable de la façon dont ses informations sont présentées sur Internet, et doit s'assurer que les mesures nécessaires ont été prises pour éviter toute déformation ou mauvaise interprétation de ce contenu.

2.4 L'intermédiation financière

2.4.1 Les organismes carte bancaire (porteur et commerçant).

La carte bancaire est un moyen très diffusé pour le payement des achats dans le cadre du commerce électronique. L'intermédiation « carte bancaire » doit fournir au vendeur la sécurité que le paiement de l'achat sera effectivement honoré et au client la protection des informations nécessaires au paiement, évitant le débit frauduleux lié aux informations transmises dans la transaction.

Un protocole a été défini par les principaux émetteurs de cartes bancaires (Visa et Master Card), le SET. Une version amélioré avec utilisation de Carte à Puce a été définie en France : le C-Set.

Ces deux protocoles établissent une relation sécurisée entre le client, le site commercial et la banque.

Mais rien ne permet de dire aujourd'hui que ces protocoles s'imposeront comme principal moyen de paiement dans le cadre du « commerce électronique ».

2.4.2 Les intermédiaires « cash » et le porte-monnaie électronique.

Ces institutions permettent aux « clients » de déposer une somme d'argent chez eux et obtenir des « jetons » pouvant être utilisées chez les « vendeurs » acceptant ce type de paiement.

Ce moyen est particulièrement adapté aux « micro paiements » (sommes très faible), pour lesquels le coût d'une transaction carte bancaire serait prohibitif.

L'intermédiaire doit assurer aux vendeurs le recouvrement des achats du client et aux clients le débit uniquement des jetons réellement utilisés. De plus, le « chargement » des porte-monnaie se faisant normalement à partir d'une carte bancaire, il doit assurer la protection des informations correspondant à cette transaction. Enfin, il doit assurer la protection des données personnelles concernant le client.

2.4.3 Les transactions de paiement dans un cadre de partenariat.

De manière générale, ce type de transactions n'inclue pas de paiement en ligne. La forme du débit est préalablement concertée entre le vendeur et l'acheteur. Ce qui compte ici est la non-répudiation de la transaction et des montants d'argent qui y sont inclus.

Ceci est pris en compte dans les normes du EDI et est abordé dans la brochure consacrée à la méthode MESSEDI disponible auprès du CLUSIF.

2.4.4 Le « Four Corners Model ».

Les modèles de gestion des transactions entre les partenaires et plus généralement d'entreprise à entreprise sont aujourd'hui clairement insuffisants pour un essor du commerce électronique B to B. En particulier, étant donnée les sommes très importantes en jeu dans une transaction B to B, l'obtention de garanties d'authenticité de l'identité et de non-répudiation de la transaction est essentielle.

Le modèle à trois acteurs (PKI, client, fournisseur) n'offre pas de moyens réellement pratiques et faciles à mettre en œuvre pour répondre à cette attente. En effet, le problème est ici bien plus lié aux garanties d'identité qu'au paiement.

Cependant, à bien y regarder, la transaction par carte bancaire offre aussi une identité unique et garantie (certes, à niveau très bas) : le numéro de la carte, géré par les institution bancaires. Il est donc assez naturel que des modèles où les entités financières jouent le rôle de « garant des identités » puissent être imaginés.

C'est le cas du modèle « Four corners », proposé par le groupement d'entités financières Identrus, auquel participent la plupart des grandes institutions financières françaises.

L'idée de base est que les deux acteurs de l'échange (deux entreprises) soient chacun relayés par une entité financière pour les opérations de vérification et validation. Ces quatre acteurs (les deux entreprises et leurs banques respectives) composent les « quatre coins » du modèle « Four Corners ».

De manière plus précise, pour pouvoir accomplir cette mission, les entités financières doivent se structurer selon un modèle hiérarchique, permettant entre autres d'accomplir le rôle d'autorité de certification.

Cette organisation hiérarchique permet aussi à Identrus de combler les lacunes de la norme X509 en normalisant selon son propre standard le contenu de certains champs laissés sans contenu précis par la norme X509.

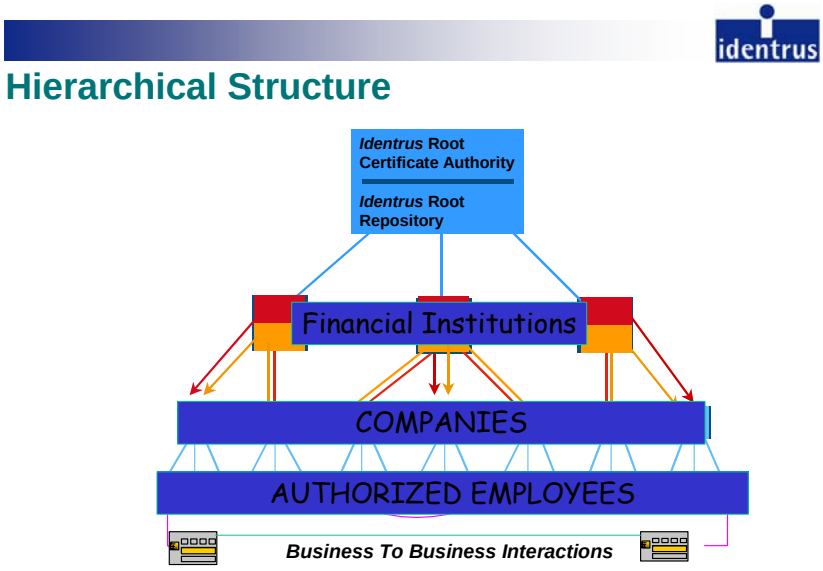

Figure 2 : organisation hiérarchique des organismes financiers proposé parr le groupement Identrus.

Une fois cette structure est mise en place, chaque employé autorisé d'une compagnie utilisant les services de l'une des institutions financières du groupement, peut faire des transactions avec tout autre employé de tout autre compagnie dans la même situation. Les institutions financières vont relayer les utilisateurs pour offrir les fonctions de vérification et validation des certificats on y apportant, en plus, des garanties propres aux institution financières (« Risk Management »).

Le modèle de fonctionnement du dispositif Identrus est décrit par le schéma suivant (« four corners »).

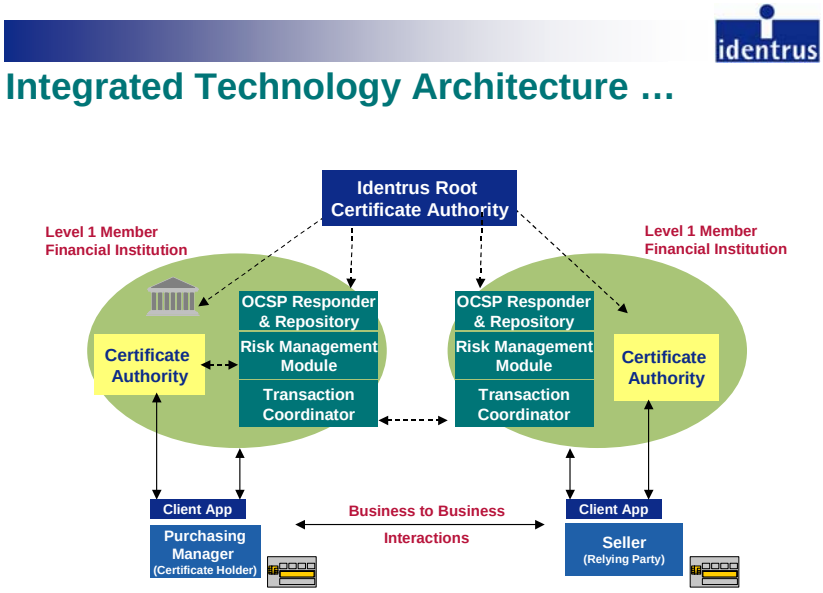

Figure 3 : Modèle "Four corners" d'Indentrus

2.4.5 Les autres modes de paiement.

La liste de modes de paiement que nous avons donné n'est pas (et ne peut pas) être exhaustive. L'absence de standards et l'importance du développement du commerce électronique avive l'imagination des différents acteurs et font naître des nouvelles méthodes.

Mentionnons ici un mode qui parait assez naturel (même s'il suscite un certain nombre de controverses) : le recouvrement des paiements par les fournisseurs d'accès (qui, en général, ont en leur possession les informations concernant le compte bancaire de l'utilisateur). De telles offres existent déjà sur le marché.

3 Les menaces particulières aux sites marchands

3.1 Les menaces

Ce chapitre essaie de compiler les principales attaques « techniques » pouvant être exécutées au détriment d'un site de commerce électronique. Rappelons qu'une attaque est destinée à compromettre la Disponibilité, l'Intégrité ou la Confidentialité des informations d'un tel site et que nous prendrons en compte ces trois aspects pour chaque type d'attaque.

Nous donnerons ici une vision très synthétique de ces attaques. Elles sont pour la plupart décrites dans d'autres brochures du CLUSIF. Pour les personnes voulant approfondir ces sujets, nous recommandons la lecture des documents « Sécurité Intranet » et « Pare-feux» rédigés par la commission Réseaux et systèmes ouverts.

Pour mieux appréhender le contexte technique de ces attaques, nous allons les classifier en trois catégories : attaques sur les protocoles de communication, attaques sur les systèmes et les applications standard et attaques sur l'information. Bien sûr, les trois niveaux peuvent être combinés mais cette « combinaison des niveaux » sera pris en compte dans d'autres chapitres plus fonctionnels.

3.1.1 Les attaques sur les protocoles de communication.

Il s'agit généralement d'exploiter les faiblesses ou anomalies des protocoles de base d'Internet (la suite TCP/IP) ou des principaux protocoles utilisés dans le commerce électronique et s'appuyant sur lui (HTTP, FTP, Telnet, SMTP…).

Dans cette catégorie d'attaques nous pouvons trouver :

- Des attaques visant à rendre indisponible le serveur ou un des services.
- L'écoute passive des communications et le rejeu.
- La substitution et la manipulation des données
- L'utilisation des protocoles non prévus ou le détournement des protocoles.

3.1.2 Les attaques sur le système et les applications standard.

En matière de système d'information, l'émergence d'un monde « ouvert et standardisé » ainsi que le fondement d'Internet en tant que support universel du commerce électronique, sont des évolutions majeures. Le nombre réduit de systèmes d'exploitation (Unix, NT et assimilés) et des applications de communication basées sur des protocoles ouverts et standard (messagerie sur SMTP, accès interactif par HTTP, consultation des basses de donnés par SQL, etc.) ont permis aux éditeurs de produire à un prix raisonnable des outils de construction de sites de E-commerce.

Mais cette standardisation facilite aussi l'élaboration de scénarios et d'outils qui permettent d'exploiter les faiblesses propres soit à ces applications standard, soit à la mise en œuvre de cette application sur un type de système, par un constructeur ou par un éditeur.

Cependant, les menaces les plus fréquentes ne correspondent pas à cette exploitation des faiblesses mais à la recherche et à l'exploitation de mauvaises configurations de ces services sur un site donné. Ces mauvaises configurations ont généralement pour cause des erreurs ou la méconnaissance des « subtilités » de l'installation des systèmes employés et des applications standard, lorsque l'on se place dans un contexte d'exposition vers Internet en général et dans le cadre du Commerce Électronique en particulier.

Nous trouvons dans cette catégorie :

- des attaques sur des services réseaux non utilisés et non ou faiblement protégés ;
- des attaques sur la disponibilité du service par utilisation des bugs des applications ;
- des attaques visant à accéder au Système d'Information de l'entreprise.

3.1.3 Les attaques sur les informations.

C'est l'objectif principal des attaques. Sauf dans le cas des attaques visant à rendre indisponible le site, le principal objectif des attaques des catégories précédentes est d'atteindre les informations relatives au commerce électronique pour obtenir un profit, soit par la divulgation, soit par la modification de ces informations. Mais des motivations plus « complexes », telles que la modification des informations pour atteindre l'image de marque de la société, ne doivent pas être sous-estimées.

Nous trouverons dans cette catégorie :

- les attaques à la disponibilité du site par saturation ou par manipulation des informations ;
- les attaques visant à une appropriation illégale des informations présentes sur le site et ne devant pas être divulguées ;
- les modifications malveillantes des informations affichées sur un site afin de désinformer les clients ou de compromettre la responsabilité civile des propriétaires ou exploitants ;
- les modifications de contenu des transactions visant un bénéfice direct.

3.2 Typologie des attaques sur le e-commerce

La classification « théorique » des menaces que nous venons de faire se décline en pratique selon diverses attaques techniques contre les site de commerce électronique.

3.2.1 Écoute passive et rejeu

L'écoute passive suivie d'un rejeu est une technique permettant de s'authentifier sur un serveur en réutilisant les paramètres d'authentification d'un tiers.

Cette attaque consiste à écouter les communications réseau par un moyen passif, c'est à dire n'agissant pas sur les communications. Le but est généralement d'en extraire les identifiants et authentifiants utilisés. Il peut s'agir de mots de passe transmis en clair, mais aussi d'autres techniques d'authentification plus élaborées. En renvoyant immédiatement le couple (identifiant, authentifiant) écouté, le pirate peut se connecter au serveur, déjouant ainsi les techniques d'authentification.

3.2.2 Substitution ou manipulation de données

La substitution ou la manipulation de données est une technique de piratage consistant à envoyer au serveur de fausses informations ayant l'apparence de vraies. Le but recherché peut être de réaliser une attaque en déni de service (*cf. infra*), par dépassement de tampon par exemple, mais aussi de générer une transaction dans l'intérêt de l'acheteur.

Par exemple, si la boutique en ligne utilise des requêtes HTTP POST afin de faire parvenir au serveur un bon de commande, et que cette requête contient le prix des articles commandés, il est facile de générer artificiellement une requête POST dans laquelle les prix ont été modifiés. Le pirate est alors en mesure de faire son prix !

3.2.3 Virus

Un virus informatique est un programme qui possède la faculté de créer des répliques de lui-même (on parle de « programme auto-reproducteur ») au sein d'autres programmes ou sur des zones système.

L'attaque virale d'un serveur web est relativement rare. Elle est toutefois possible, que ce soit par l'intermédiaire du webmaster (préalablement contaminé) ou par attaque pirate. Les conséquences de ce type d'attaque sont doubles :

- si le virus est placé dans du code s'exécutant sur le serveur (script CGI, fichier de script exécuté coté serveur, etc.), celui-ci est susceptible de subir les même dommages qu'une machine ordinaire (perte des fichiers, propagation du virus, etc.) ;
- si le serveur propage le virus chez des visiteurs, la responsabilité civile du commerçant peut alors être engagée.

3.2.4 Chevaux de Troie

Un cheval de Troie est un programme informatique contenant une fonction cachée, inconnue de l'utilisateur. Cette fonction est notamment utilisée afin de s'introduire dans l'ordinateur et consulter, modifier ou détruire des informations. Ces programmes sont ainsi utilisés pour récupérer des mots de passe, voire pour prendre le contrôle intégral à distance de la machine.

Il existe aujourd'hui de nombreux programmes de piratage fonctionnant selon le principe du cheval de Troie. Ces programmes pourront permettre au pirate de prendre le contrôle complet de la machine à distance, ou encore d'utiliser la machine comme relais pour une attaque élaborée vers une cible secondaire.

Les attaques en déni de service réparties (*cf infra*) fonctionnent à l'aide d'un programme apparenté aux chevaux de Troie. C'est alors la machine piratée qui semblera attaquer la cible finale. La responsabilité de l'entreprise peut dans ce cas être recherchée. Il est donc fondamental de se protéger afin de ne pas servir de relais.

3.2.5 Répudiation

La répudiation consiste à nier avoir participé à une transaction. Par exemple, si le client peut nier avoir fait un achat, et refuser le paiement. Selon les systèmes de paiement utilisés, le commerçant peut alors ne pas être payé, alors que la marchandise aura été livrée.

Même si la répudiation est parfois légitime pour le client (dans le cas où il n'aurait réellement pas passé la commande), le vendeur subit dans tous les cas une perte sèche, à moins que le système de paiement ne garantisse le recouvrement.

La signature électronique ayant désormais valeur légale, il est de l'intérêt du commerçant de se prémunir contre les risques de répudiation.

3.2.6 Déni de service

Le déni de service est un type d'attaque informatique. Il consiste à rendre un service informatique (par exemple, un serveur Internet) indisponible.

Une méthode d'attaque en déni de service couramment utilisée actuellement est l'attaque répartie. Celle-ci est présentée ci-dessous.

Une autre méthode couramment employée lors des attaques en déni de service est le « dépassement de tampon ». Elle consiste à envoyer au serveur un message plus grand que la

capacité de réception du serveur. Ce message peut être fabriqué à l'aide des techniques de substitution et de manipulation de données (*cf supra*).

3.2.6.1 Le déni de service réparti (DDoS)

De manière générale, il existe de nombreuses manière de mener ce type d'attaque. L'une des techniques les plus élaborées est l'attaque répartie (Distributed Denial of Service, ou DDoS). Cette technique a été employée à plusieurs reprises au début de l'année 2000 contre des serveurs de commerce électronique américains

Une étude de ce type d'attaque et des moyens de protection est disponible sur le site du CLUSIF.

Schématiquement, une attaque en déni de service répartie consiste à générer des flux d'information adressé à la machine cible depuis un grand nombre de machines relais situées un peu partout sur le réseau Internet.

Un certain nombre d'outils de piratage permettent de réaliser cette attaque. Ils fonctionnent globalement de la manière suivante :

- Le pirate utilise un programme spécial sur sa machine, que nous appellerons "client de contrôle" ;
- Ce programme de contrôle dirige à distance un certain nombre d'agents de contrôle ;
- Ces agent lancent des flux de paquets destinés à une même cible.

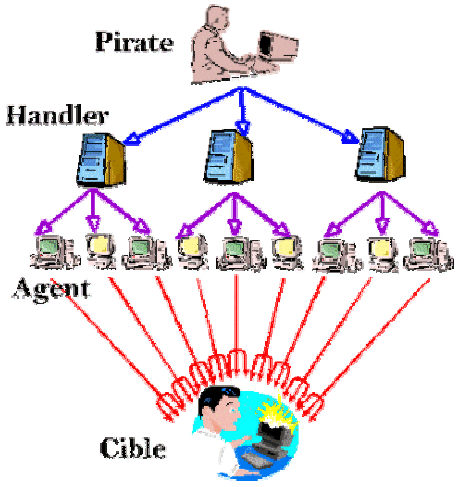

Figure 4 : fonctionnement d'une attaque en déni de service répartie.

Sans être un expert en lutte contre le déni de service, des mesures simples peuvent être prises :

- Filtrer correctement le trafic.
- Être rigoureux dans l'application du concept "tout ce qui n'est pas autorisé est interdit".
- Brider le trafic au-dessus d'un certain seuil. Ainsi, le serveur ne sera pas saturé, et ne plantera pas. L'accès au site sera ralenti, mais statistiquement, les paquets émanant de vrais clients arriveront à passer ; le service restera donc disponible.

Des techniques spécifiques existent aussi au niveau du paramétrage des routeurs. Nous vous conseillons de prendre contact avec votre fournisseur pour obtenir le détail des règles à mettre en œuvre sur votre matériel.

3.2.7 Spamming...

Le *spamming* consiste en l'envoi massif de courriers électroniques non sollicités, généralement à tendance commerciale ou pseudo-commerciale.

Pour le commerçant, « spammer » ses clients serait plutôt une mauvaise idée : cela risque de les faire fuir, et cela portera dans tous les cas préjudice à l'image de l'entreprise. Toutefois, l'attaque dont nous parlons ici est le *spamming* réalisé par un tiers à l'insu du commerçant.

Cette attaque est possible si le « spammeur » parvient à récupérer la liste des clients en piratant le serveur web, ou si le commerçant gère une liste de diffusion permettant à un tiers d'envoyer un message. De nombreux commerçants électroniques mettent en place une liste de diffusion, qui leur sert par exemple à avertir leurs clients de nouveautés ou de promotions. Il est fondamental que le logiciel de gestion de liste soit paramétré de sorte que seul le propriétaire de la liste, c'est-à-dire le commerçant, ait la possibilité d'envoyer un message sur la liste.

De la même manière, le commerçant devra prendre soin que ses passerelles de messagerie soient configurées de manière à interdire le *mail-relay* (possibilité pour un tiers de faire partir du courrier depuis le serveur de messagerie de l'entreprise). En effet, les serveurs ouverts au *mail-relay* sont utilisés prioritairement par les « spammeurs » pour se camoufler.

3.3 Conséquences financières et juridiques d'attaques pour un site de e-commerce

3.3.1 Fraude

Un point à anticiper lors de la mise en place d'un site marchand est la fraude. Celle-ci peut être de plusieurs type : il peut s'agir d'un client achetant un produit pour un prix incorrect, d'un client achetant un produit en utilisant les moyens de paiement d'un tiers, d'un « client » réussissant à faire passer un ordre de livraison sans le paiement correspondant, etc.

Les sources de fraudes peuvent avoir plusieurs origines : défaillance dans la conception du site qui permet, en envoyant les bonnes informations au serveur, de générer des commandes frauduleuses, mais aussi usurpation de moyens de paiement valables.

3.3.2 Frais de recouvrement / transport

Une mauvaise sécurisation du processus de prise de commande et/ou de paiement peut entraîner des frais de recouvrement et de transport.

Les frais de recouvrement auront lieu lorsque le paiement correspondant à la commande sera difficile à obtenir. Les frais de transport auront lieu en cas de livraison d'une commande à une mauvaise personne, voire à une personne n'ayant rien commandé !

S'il s'agit là de risques rencontrés dans toute forme de vente par correspondance, cela ne signifie pas qu'il faut les oublier quand on fait du commerce électronique !

3.3.3 Perte de marchandise

Enfin, dans le cas où le recouvrement d'une créance s'avérerait impossible, il pourra y avoir perte sèche de la marchandise livrée.

3.3.4 Perte financière de l'entreprise

La confidentialité, souvent mise en avant, n'est pas le seul point à surveiller sur un site de commerce électronique. La disponibilité doit aussi être assurée : si le site n'est plus joignable, les clients ne peuvent venir acheter. Ils sont alors susceptibles de se tourner vers vos concurrents.

Ainsi, une mise en indisponibilité d'un site web durant « seulement » trois heures a pu récemment coûter jusqu'à 500 000 $. Il s'agit là de la perte directement due à la mise en indisponibilité du site.

3.3.5 Perte financière des clients/partenaires

Dans le cas de commerce inter-entreprises, une défaillance de la sécurité d'un site marchand peut entraîner une perte financière non seulement pour l'entreprise propriétaire du site, mais aussi pour ses partenaires.

Prenons l'exemple fictif d'un site vendant des automobiles sur Internet, servant de vitrine à un réseau de concessionnaires. Si la sécurité du site de l'entreprise est défaillante, la perte financière concernera non seulement l'entreprise propriétaire de la boutique virtuelle, mais aussi le réseau de concessionnaires partenaires de l'opération.

3.3.6 Espionnage industriel

Un site de commerce électronique gère nombre d'informations commerciales, telles que le fichier client, mais aussi le catalogue, qui sont susceptible d'intéresser les concurrents de l'entreprise. Il s'agit donc d'une cible privilégiée d'espionnage industriel.

Si 80% des informations utilisées dans le cadre d'espionnage industriel sont des informations publiques, un site marchand est une source particulièrement intéressante pour la veille concurrentielle.

Plus encore, les informations confidentielles qui y sont stockées, telles que le fichier des clients, de leurs coordonnées et de leur « profil d'acheteur » sont des informations devant être protégées.

La sécurité d'un site de commerce électronique doit donc assurer la confidentialité de ces données.

4 Mesures génériques à la sécurisation d'un site web

4.1 Introduction

Il n'y a pas de solution simple et immédiate pour sécuriser un site web. Il faut donc adopter la démarche de sécurisation habituelle : étudier le problème de manière globale et appliquer des mesures homogènes à tous les niveaux de l'architecture système.

Ainsi l'architecture de sécurité destinée à la protection du serveur web doit inclure des mesures de sécurité techniques à tous les niveaux du système :

- protection au niveau du serveur ;
- protection au niveau du réseau ;
- protection au niveau de l'application.

Par ailleurs, le contenu des pages mises à disposition doit respecter les exigences de sécurité non couvertes par les mesures techniques :

- les obligations légales (droit d'auteur...) ;
- la non divulgation d'informations confidentielles ou privées (informations bancaires, dossier médical…).

4.2 Protection au niveau du serveur

4.2.1 Paramétrer le système d'exploitation

La protection du serveur web et de ses données est impossible tant que le système d'exploitation sous-jacent n'est pas sécurisé. Pour cela, il faut des mesures de sécurité spécifiques concernant, la gestion des utilisateurs, des processus, des systèmes de fichiers...

Les fonctions de sécurité standard du système d'exploitation peuvent être utilisées, il est cependant conseiller d'ajouter des produits de sécurité supplémentaires pour renforcer les fonctions standard (voir le document CLUSIF : « Sécuriser Unix »).

Des comptes possédant des niveaux de privilèges différents seront attribués aux administrateurs et développeurs en fonction de leurs besoins.

Le serveur web sera installé, dans la mesure du possible, sur une machine différente des autres applications (ex : serveur de messagerie, serveur de cache…) afin d'éviter les vulnérabilités liées à ces services.

Il faut activer les fonctions d'audit et de journalisation afin de tracer les actions sur le serveur.

4.3 Protection au niveau du réseau

Un équipement de filtrage (de type firewall) peut être utilisé afin de limiter les flux réseau ouverts depuis l'extérieur en direction du serveur web. Le firewall permet de réaliser un filtrage par service des accès entrants, et limite ainsi les risques auquel est soumis le serveur web. Une autre fonction importante du firewall est la journalisation du trafic.

La fonction de sécurité réseau essentielle est le filtrage (« filtrage IP »), cependant une fonction détection d'intrusion peut également être installée. Il s'agit d'une fonction de sécurité annexe. Celle-ci est de plus en plus souvent intégrée au sein même de l'équipement de filtrage. Elle permet notamment de générer des alertes si elle repère dans le trafic réseau la « signature » d'une attaque déjà connue ou d'un comportement suspect (à la manière des anti-virus).

L'architecture réseau retenue pour l'interconnexion est capitale. Le réseau doit être cloisonné pour protéger le réseau interne en cas de compromission du serveur web. On peut utiliser le principe des architectures 3-tiers tel que l'illustre le schéma ci-dessous. Le schéma présente une architecture à trois niveaux, mais on peut définir des niveaux intermédiaires supplémentaires.

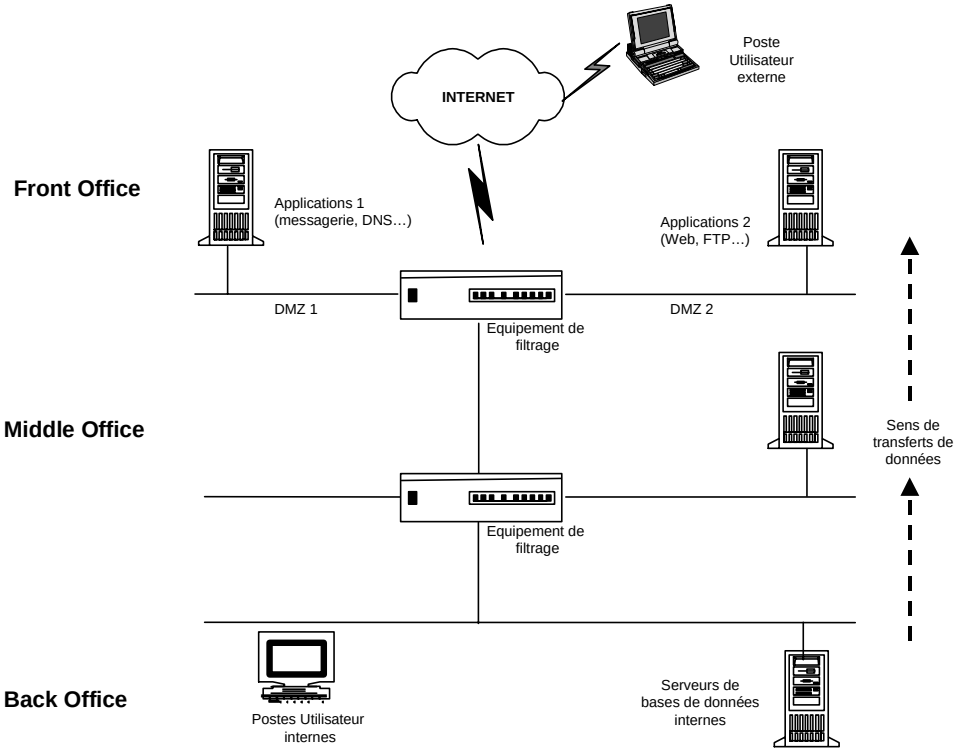

Figure 5 : exemple d'architecture réseau 3-tiers.

L'écriture des données s'effectue toujours de l'intérieur vers l'extérieur. Il ne doit pas y avoir de modifications possibles du contenu des données de l'extérieur vers l'intérieur

4.4 Protection au niveau de l'application

L'application est constituée par le logiciel serveur web lui-même.

4.4.1 Contrôler l'intégrité des données

Concernant les serveurs web, un objectif majeur est de protéger le contenu des pages mises à la disposition des clients et donc de garantir l'intégrité des données du serveur. Si les pages sont statiques, la solution la plus simple consiste à calculer la signature des fichiers correspondants et à vérifier qu'elle ne varie pas au cours du temps, du moins tant qu'une nouvelle version n'a pas été livrée.

Par ailleurs, il est nécessaire de procéder au contrôle anti-virus des fichiers (si le serveur est Unix il faut au moins vérifier les fichiers bureautiques transmis).

4.4.2 Séparer les rôles

Il faut différencier les rôles des intervenants sur le serveur et distinguer notamment l'administrateur du serveur web, les responsables de la mise à jour des pages...

La séparation en deux applications, l'une pour la production des pages, l'autre pour la diffusion aux clients, est vivement conseillée. Ces deux logiciels peuvent tourner soit sur la même machine ou mieux sur deux machines différentes pour des raisons de disponibilité.

Il faut contrôler les accès au compte ou au serveur d'administration.

4.4.3 Journaliser

Il faut activer les fonctions d'audit et de journalisation afin de tracer les actions et mémoriser les connexions des clients.

4.4.4 Inhiber les options dangereuses

Les options dangereuses dépendent de l'application choisie. Il est important de paramétrer correctement son serveur web, un certain nombre de fonctionnalités apportant leur lot de vulnérabilité. Par exemple, les options suivantes seront à activer en connaissance de cause : following links, automatic directory listing, server side includes (files include), scripts et programme exécutés coté serveur (ASP, PHP, CGI…), user-maintained directories…

Dans le même esprit, les droits de lecture/écriture/exécution positionnés pour chaque répertoire ou fichier au sein du serveur web devront être soigneusement paramétrés (ne pas autoriser l'exécution sur un répertoire permettant aux visiteurs de déposer des fichiers, par exemple !).

4.4.5 Maîtriser les programmes CGI

Eviter les programmes CGI (Common Gateway Interface) s'ils ne sont pas absolument nécessaires.

Si de tels programmes sont utilisés, il faut être vigilant dans la conception de programmes CGI. Leurs failles sont fréquemment exploitées par les individus hostiles, car ils peuvent permettre l'exécution de commandes arbitraires sur le serveur. La plupart des vulnérabilités des serveurs web sont issues de cette faiblesse.

4.4.6 Utiliser les fonctions de chiffrement

Les échanges nécessitant un certain niveau de confidentialité doivent utiliser les options de transfert sécurisé basé sur le chiffrement (SSL, HTTPS…)

4.4.7 Contrôler les accès utilisateur

L'accès réservé à certaines parties du serveur peut être mis en place le cas échéant. Cela permet la mise en place d'un contrôle d'accès par mot de passe pour que les utilisateurs n'aient accès qu'aux données qu'ils ont le droit de consulter. Dans certains cas, des solutions d'authentification plus élaborées seront retenues (mot de passe à usage unique, utilisation de certificats…).

4.5 Disponibilité et Sûreté de fonctionnement

Concernant la disponibilité du serveur web, les règles classiques s'appliquent :

- effectuer des sauvegardes régulières ;
- dimensionner correctement le serveur en fonction du nombre de client ;
- éviter les pages comportant beaucoup d'images ;
- utiliser des systèmes d'équilibrage de charge (" load-balancing ") ;
- utiliser des systèmes à tolérance de panne ;
- utiliser la redondance des éléments critiques…

En fonction du besoin, il peut être intéressant de d'avoir en redondance le serveur d'hébergement, voire le fournisseur d'accès à Internet.

5 Besoins de sécurité propres aux sites marchands

Comme le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) n'a pas été conçu pour garantir la sécurité des services de communication sur Internet (la version 6 du Internet Protocol inclura certaines fonctions orientées vers la sécurité), il est nécessaire de recourir à d'autres technologies de sécurisation pour résoudre les problèmes de plus en plus nombreux dans ce domaine.

Les infrastructures électroniques sécurisées reposent essentiellement sur SSL (Secure Socket Layers), SET (Secure Electronic Transactions) et S/MIME (Secure Multipurpose Internet Mail Extensions). Ces protocoles, qui sont des normes de fait pour les entreprises, sont à la base d'une large gamme de services de sécurité (signatures électroniques, vérification de l'intégrité, authentification et chiffrement de messages).

Les logiciels de navigation les plus couramment utilisés (Netscape Navigator et Microsoft Internet Explorer) exploitent ces possibilités et font appel à des serveurs compatibles SSL proposés par les principaux fournisseurs. Des fonctions de sécurité supplémentaires exigées par des applications informatiques spécifiques peuvent être intégrées dans d'autres API (interface de programme d'application), scripts Javascript et applets Java, Visual Basic, C/C++ ou d'autres langages de programmation.

5.1 Authentification des utilisateurs

Lors d'une transaction en ligne, le site doit pouvoir authentifier la personne qui se connecte lorsqu'il s'agit d'accéder à de l'information à usage restreint ou lorsque la validation d'une transaction nécessite de vérifier les droits de l'internaute; en effet un utilisateur d'un service de banque en ligne se doit d'être authentifié par la banque. On remarquera que l'authentification précède toujours une opération (transaction) de valorisation de l'information. Il peut s'agir de valeur financière (transaction bancaire) ou de valeur indirecte liée à l'information elle-même (accès aux ayants droit uniquement).

Les protocoles comme SSL ou TLS permettent une authentification mutuelle entre clients et serveurs grâce à l'utilisation de certificats X509. Un certificat peut contenir une large quantité d'informations qui détermine précisément son usage. Quelques informations supplémentaires seront toujours requises, par exemple l'algorithme à utiliser ou le certificat de date d'expiration. D'autres informations pourraient être volontaires et dépendraient du but dans lequel le certificat est utilisé et du niveau de confiance requis.

Exemples de contenu d'un certificat:

• nom ou pseudonyme du signataire
• nom de l'AC
• clé publique du signataire
• algorithme
• type de clé
• profession
• position occupée au sein d'une organisation (par exemple complémentaire dans un "partenariat limité", vice-président exécutif d'une société)
• qualifications, licences (par exemple avocat, docteur, entrepreneur de transport)
• autorisations officielles (par exemple permis de conduire)
• limites en matière de responsabilité (limites légales, par exemple "commanditaire" ou "partenariat limité")
• solvabilité (par exemple assurance, dépôt)
• date d'expiration du certificat

Cela mène à une variété de classes de certificats. Par exemple, un certificat utilisé pour autoriser un transfert financier important entre deux banques nécessitera un degré de confiance élevé, alors qu'un autre utilisé pour valider un achat personnel d'un montant limité ne nécessitera pas un degré de confiance comparable.

Le degré de confiance attribué au certificat et donc à la clé privée de son propriétaire peut être également influencé par les conditions de conservation de cette clé privée.

Dans la plupart des logiciels du commerce utilisés pour effectuer des transactions électroniques(Netscape Communicator, Interner Explorer,…) les clés privées des utilisateurs sont stockées sous une forme de fichier chiffré par un mot de passe. Ce procédé de stockage de la clé privée est réputé comme présentant une résistance peu élevée aux menaces virales notamment. Ceci signifie que plus l'exigence de confiance sur l'authentification est élevée, plus le niveau de résistance du processus de stockage de la clé privée doit être élevé.

Ainsi, dans les pays européens où la signature électronique est légalement reconnue, le moyen de stockage des clés privées utilisées pour effectuer une signature électronique, c'est à dire une authentification, doit avoir été certifié selon les normes de sécurité ITSEC E4 ou Critères Communs-EAL5.

5.2 Confidentialité des échanges

Il s'agit de garantir le secret de l'information transmise ou archivée. En général, on utilise le chiffrement au moyen d'une clé symétrique. Tout, du courrier électronique aux commandes d'administration d'un ordinateur à distance, peut être ainsi protégé sous une forme chiffrée.

Dans le cadre d'une transaction électronique sur Internet ou sur un réseau virtuel privé, le besoin de confidentialité est motivé par la nécessité de protéger des informations personnelles (n° de carte bancaire, n° de compte, montant et nature d'un achat,…) ou des informations à caractère industriel ou commercial (reporting financier, commandes en ligne,…).

Les logiciels serveurs e-commerce standards sur le marché proposent la mise en œuvre du protocole SSL. Il permet d'assurer une confidentialité entre le browser de l'internaute et le serveur e-commerce et assure l'internaute de l'identité su serveur. La mise à disposition de cryptographie 128 bits sur les browsers du marché, suite à l'assouplissement des lois d'exportation, devrait permettre d'assurer un bon niveau de confidentialité.

5.3 Non répudiation des transactions

La cryptologie s'intéresse aussi à d'autres problèmes dont l'importance va croissant, comme la non-répudiation, garantissant que l'auteur d'un message ou d'un document ne puisse pas nier l'avoir écrit et, le cas échéant, transmis.

Le principe de la non-répudiation est mis en œuvre, notamment, lors d'un paiement avec une carte bancaire à puce. Selon la version du terminal de paiement et de la carte, une séquence de 8 à 16 chiffres hexadécimaux figurent sur le ticket imprimé par le terminal. Cette séquence peut être utilisée pour démontrer la réalité de la transaction en cas de contestation.

Le processus de non-répudiation nécessite la mise en œuvre d'éléments secrets; symétriques dans le cas des cartes bancaires, asymétriques dans les transactions en ligne. La validité du processus implique que les clés utilisées pour prouver la réalité d'une opération, soient totalement à l'abri d'une compromission.

En effet même si une clé privée a été allouée à une personne, cela ne prouve pas que cette personne a réellement signé un document donné. Alors que dans une situation normale, le propriétaire de la clé signe le document, une signature numérique ne peut être associée qu'à une clé privée déterminée. Cette présomption est seulement valable dès lors qu'il est établi que le propriétaire de la clé secrète exerce un contrôle total et exclusif sur celle-ci.

Exemple: Au contraire des signatures conventionnelles, où le signataire signe avec sa propre main, les signatures numériques permettent à une tierce personne - autorisée ou non - de signer un document si elle est en possession de la clé privée. C'est ce qu'on appelle la délégation « non révélée ».

L'allocation de clé est néanmoins possible s'il peut être légalement présumé que le propriétaire de la clé signe lui-même. Dans ce cas, le propriétaire pourrait souhaiter être juridiquement responsable uniquement jusqu'à un certain degré (par exemple dans une certaine limite, comme pour une carte de crédit). Des règles juridiques appropriées devraient donc être prises en considération par les offreurs de service.

5.4 Intégrité des données

Il est particulièrement important que, dans toute négociation et accord contractuel, on puisse vérifier qu'aucune modification du document électronique n'a été faite. De même pour toutes les transactions en ligne BtoB ou BtoC, telles que commandes et transactions engageant la responsabilité financière ou légale des parties.

Une société de bourse en ligne prendrait aujourd'hui de gros risques en n'étant pas en mesure d'assurer que l'ordre transmis par l'abonné au service de courtage en ligne correspond bien à l'ordre reçu.

La signature numérique sera le moyen le plus couramment utilisée dans ce cas. Ce service sera ainsi couplé avec le service de non-répudiation.

5.5 Paiement

Le paiement est généralement l'aboutissement de la transaction en ligne sur un serveur e-commerce. Le déploiement de ces serveurs dans un monde sans frontière doit autoriser le mode de paiement aujourd'hui le plus largement répandu, mais aussi le moins sûr, qui consiste à transmettre un numéro de carte bancaire. Les sites marchands devront alors veiller à ce que ces numéros ne soient pas stockés sur le serveur assurant les transactions sur Internet, ou en tout état de cause soient stockés chiffrés pendant le période de réalisation du paiement.

Si le commerçant peu s'assurer de la validité du moyen de paiement avant la livraison, il est difficile à un client d'un service à distance de s'assurer de la réalité de ce service. En effet, à ce jour, seul le certificat délivré au site marchand par une autorité de certification permet de vérifier son identité. Encore faut-il que le paiement soit validé sur un²e liaison sécurisée par SSL.

Malheureusement un nom sur un certificat ne donne aucune garantie de bonne mœurs. En réponse à ce soucis, on voit aujourd'hui apparaître labels de qualité de service afin de rassurer l'internaute acheteur sur le bon déroulement du processus de vente. La confiance du client dans la marchand est alors basée sur la réputation des organismes de labellisation et la reconnaissance de leur probité par le public.

La sécurité des paiements sur Internet devrait être bientôt une réalité avec l'apparition du service CyberComm, qui est une adaptation du protocole SET à la carte à puce. Ceci devrait permettre à cette solution française, née de l'expérience de la carte bancaire à puce sur le marché, de ne pas être limitée au seul Hexagone. Son succès dépendra de la volonté des banques à distribuer des lecteurs CyberComm à leurs clients, ces lecteurs faisant partie intégrante du protocole.

6 Etude de cas

Au cours des chapitres précédents, nous avons recensé les acteurs du commerce électronique (chapitre 2), puis identifié les menaces et les risques portant sur un site web marchand (chapitre 3). Nous avons ensuite présenté les mesures de sécurité à notre disposition pour maîtriser ces risques (chapitres 4 et 5). Au cours de ce chapitre, nous allons regarder comment les mesures de sécurité permettent de réduire un risque autour d'un cas concret.

Pour cela, nous allons partir d'un exemple (volontairement simple) de site marchand, en lister les fonctionnalités, et pour chaque fonctionnalité présenter quelques menaces et quelques parades correspondantes.

Les solutions présentées ici ne sont pas exhaustives, mais ont pour but de donner un aperçu des outils dont dispose le concepteur du système pour l'aider à le sécuriser. Des outils présentés comme réponse à une menace dans un contexte donné peuvent servir pour traiter d'autres menaces (ainsi, nous verrons que l'exemple du protocole SSL est utilisé dans plusieurs contextes). Par ailleurs, d'autres solutions existent qui permettent de traiter les problèmes posés.

Enfin, ce chapitre pourra donner l'impression d'être un catalogue de solutions. C'est un peu sa vocation. Mais il ne faut pas perdre de vue qu'une solution mal intégrée répond mal au besoin, et que les outils techniques ne traitent pas tous les problèmes.

Par conséquent, la mise en place d'un site marchand devra toujours partir d'une analyse des risques afin de déterminer quelles sont les menaces portant sur le système, et quelles sont les solutions techniques et organisationnelles les plus adaptées.

Ce chapitre présente des solutions techniques. Le responsable sécurité ne devra toutefois pas oublier que la technique n'est qu'une petite partie de la problématique « sécurité ». Un effort important devra être apporté aux aspects organisationnels et procéduraux. En effet, la mise en place d'une batterie d'outils, aussi complète soit-elle, ne protégera jamais de l'erreur humaine, source de nombreuses failles de sécurité sur les sites de commerce électronique.

6.1 Le cas étudié

La société Clusifrance[1] est une société de prêt à porter. Son siège est à La Défense en région parisienne, et son usine est à Nîmes dans le sud de la France.

Afin d'apporter un meilleur service à ses clients, Clusifrance a décidé de créer un site web sur lequel les internautes pourront consulter le catalogue et commander en ligne des vêtements à leurs mesures (technique dite de « demi-mesure »).

[1] Cette société est inventée de toute pièce pour les besoins du cas. Toute ressemblance avec un cas réel existant ou ayant existé est purement fortuite. Cependant, le cas est tout de même conçu pour que tout le monde s'y reconnaisse un peu !

Le site « Clusifrance on-line » comprend donc les fonctionnalités suivantes :

- le catalogue de présentation des vêtements ;
- un module d'achat en ligne ;
- une base de données stockant les informations sur le client (ses coordonnées, sa taille, ses modes de paiement, etc.) ;
- un couplage avec le système d'information de l'entreprise pour lancer la production d'un vêtement sur mesure ;
- un couplage avec le système d'information de l'entreprise pour mettre à jour le catalogue ;
- un outil d'analyse statistique du comportement des visiteurs ;
- hébergement externe à l'entreprise, chez un hébergeur professionnel.

6.2 Protection générale du site

6.2.1 Le contexte

Un site de commerce électronique est, entre autres, un site web.

Dans le commerce traditionnel, le propriétaire d'un magasin prend soin de sa facilité d'accès. Il choisit un bon emplacement, aménage un parking, et met en place des panneaux indiquant l'emplacement de la boutique s'il y a des travaux devant.

De même qu'une boutique « en dur » doit être facilement accessible par les clients, un site web marchant doit avoir une excellente disponibilité : si le site est inaccessible, les clients ne peuvent pas venir le consulter, et encore moins y faire des achats.

6.2.2 La menace

La menace que nous allons traiter ici est le déni de service, qu'il soit accidentel ou malveillant.

6.2.3 L'environnement physique

De manière générale, un site internet doit être hébergé dans un environnement sécurisé. La plate-forme d'hébergement devra donc assurer un niveau de sécurité physique convenable : protection incendie et inondation, climatisation, alimentation électrique, accès physique sécurisé.

6.2.4 L'environnement logique

Une plate-forme d'hébergement doit aussi garantir un niveau convenable de sécurité logique des sites hébergés : sauvegardes des sites web et de la configuration des machines, contrôle d'accès logique (en particulier firewall), protection antivirus, supervision des tentatives de piratage, etc. Des audits doivent être menés régulièrement sur ces systèmes (audits « classiques » et tests d'intrusions peuvent être menés en complément l'un de l'autre).

6.2.5 Configuration du serveur

Une mauvaise configuration du serveur d'hébergement est souvent la source d'une faille de sécurité. L'administrateur de la machine devra donc paramétrer avec attention le serveur. Les services tournant dessus devront être réduit au minimum et correctement configurés.

Les droits d'accès, de lecture, d'écriture, d'exécution… devront être eux aussi paramétrés avec soin sur le système d'exploitation aussi bien que pour chacun des services tournant sur la machine.

6.2.6 La disponibilité

Le site de commerce est la boutique de Clusifrance. Si cette boutique est fermée, Clusifrance ne vend plus. La plate-forme d'hébergement doit donc être conçue pour obtenir la meilleure disponibilité possible pour les sites hébergés. Des techniques de répartition de charge et de tolérance de panne pourront être prévues pour ce qui concerne la disponibilité des machines. De même, les accès télécoms devront être redondants. Des outils de supervision doivent être mis en place pour assurer le suivi de la qualité de service.

Enfin, il est conseillé de travailler sur deux versions du site simultanément : une version dite « de production », destinée à l'utilisation par le public, et un une version dite « de développement », destinée à la mise en place de nouvelles fonctionnalité afin de réaliser les tests d'intégration dans l'environnement définitif, mais sans prendre le risque d'occasionner des dégâts sur le site de production.

6.2.7 Sauvegarde et archivage

Comme toute plate-forme informatique, un site web, et *a fortiori* un site de commerce électronique, contient des informations qui doivent être d'une part sauvegardées, d'autre part archivées.

La sauvegarde répond à un besoin d'exploitation. Elle a une finalité de disponibilité, son but étant de permettre la récupération de données en cas de sinistre (que ce soit un accident, une erreur ou une malveillance).

L'archivage a des objectifs plus variés, possédant chacun des caractéristiques propres : archivage légal, comptable, commercial (constitution d'un fichier clients pour applications de GRC…), etc. Chacun de ces besoins a des impératifs différents en matière de durée d'archivage et de sensibilité des informations archivées.

Pour plus de détails, le lecteur pourra se reporter au document « La sauvegarde et l'archivage » disponible auprès du Clusif.

6.2.8 Plans de secours

De même que les procédures de sauvegarde et d'archivage ont été définies, des plans de secours et de continuité devront être conçus. Ces plans devront pouvoir parer au maximum de scénarios d'indisponibilité possible (défaillance de l'hébergeur, du fournisseur d'accès, du serveur d'hébergement, etc.).

6.3 Classification des informations

6.3.1 Le contexte

Un site web, marchand ou non, sert à présenter des informations. Si ce site est disponible sur Internet, il présente des informations venant de l'entreprise à des personnes extérieures à l'entreprise. Il conviendra donc de classifier ces informations afin de déterminer qui à accès à quoi.

6.3.2 Les menaces

Prenons l'exemple du catalogue des produits (qui sera repris par la suite sous d'autres aspects). Une entreprise possède généralement plusieurs catalogues de ses produits : un catalogue destiné à la production, un catalogue destiné au marketing, un catalogue destiné aux partenaires, etc. Tous ces catalogues ne sont pas publics, et certains d'entre eux seront même hautement confidentiels.

Il faut donc veiller à ce que les informations publiées sur le site soient bien des informations publiques.

6.3.3 Les solutions

Les solutions disponibles sont essentiellement organisationnelles. Les responsables du site devront établir une classification des informations, et déterminer qui a le droit d'accéder à quoi. Ils devront ensuite concevoir la procédure d'élaboration et de validation du catalogue public. Dans certains cas, cette procédure pourra être automatisée à partir des bases de données de l'entreprise. Il faudra alors veiller à la sécurité de ce système de génération automatique. Dans d'autre cas, la validation, et même parfois l'élaboration, du catalogue devront être manuelles. La sécurité des procédures de mise à jour du site devra alors être vérifiée.

6.4 Catalogue produit

6.4.1 Le contexte

Le catalogue mis en ligne présente les produits, leurs caractéristiques et leurs prix. L'internaute qui consulte ce catalogue doit pouvoir être certain que les informations indiquées sont correctes.

La législation en vigueur en France oblige les commerçants à respecter les tarifs affichés. Par conséquent, si un prix est incorrect, le client peut demander à ce qu'il lui soit appliqué tout de même.

6.4.2 La menace

Les menaces portant sur le catalogue sont :

- le remplacement du catalogue par une page placée par un pirate (« *web defacement* ») ;
- les modifications de contenu (prix, références, descriptif, etc.) ;
- le « spoofing » de site (mise en ligne d'un site similaire, que les internautes consultent en pensant être sur le site de Clusifrance, mais présentant des informations fallacieuses).

6.4.3 L'authentification de contenu

Afin de se prémunir contre la modification de contenu, des outils d'authentification de contenu peuvent être utilisés. Ces outils vérifient que le site consulté par le public n'a pas été altéré.

6.4.4 Le chiffrement SSL – certificat serveur

Utiliser un certificat serveur afin de chiffrer les communications en SSL a un rôle complémentaire au simple chiffrement des échanges : le certificat authentifie le site consulté. Ainsi, le visiteur est certain de visiter le site de Clusifrance. En fonction des informations présentées, l'entreprise pourra choisir d'utiliser SSL pour tout ou partie de son site.

Lors de la visite d'un site disposant d'un certificat SSL, le navigateur de l'internaute lui signale que le site est « sécurisé » en affichant un cadenas comme celui-ci :

-  en bas à gauche sous Netscape Navigator.
- 

en bas à droite sous Microsoft Internet Explorer.

En double-cliquant sur ce cadenas, des informations sur l'identité du site sont vérifiées :

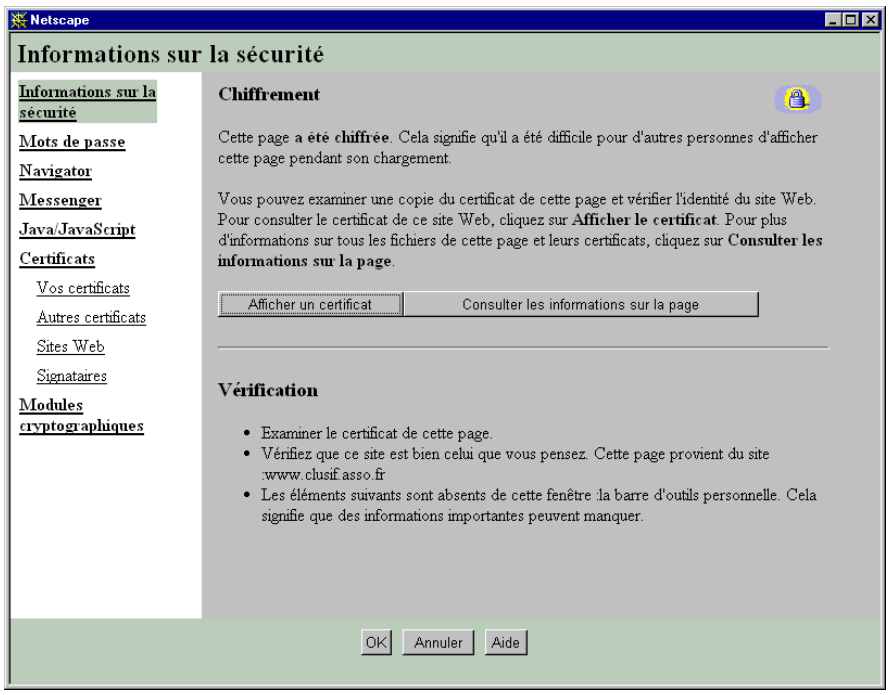

Figure 6 : vérification de l'identité de l'interlocuteur

La délivrance d'un certificat par un tiers de confiance n'est possible qu'après de nombreuses vérifications d'identité du demandeur. Par conséquent, si le site est victime d'une attaque par « spoofing », le pirate n'est pas en mesure de se faire délivrer un certificat valide pour la même adresse.

6.5 Achat en ligne

6.5.1 Le contexte

Le site « Clusifrance on line » permet à l'internaute d'effectuer des achats en ligne. Nous entendons par là que le client est en mesure de passer commande pour un produit à un tarif indiqué, puis à payer cette commande par internet.

6.5.2 Les menaces : écoute, vol d'information et répudiation

Les principales menaces portant sur l'acte d'achat concernent d'une part les moyens de paiement, d'autre part l'achat proprement dit. Ces menaces peuvent être classées en deux catégories : menaces provenant d'un des co-contractants et menace provenant d'un tiers.

La menace provenant d'un des co-contractants est typiquement la répudiation de l'acte : le client, le vendeur (et éventuellement un intermédiaire de paiement) nie sa participation à l'une ou à l'ensemble des étapes de l'achat : la commande, le paiement ou la livraison.

Les menaces émanant de tiers sont l'écoute et/ou le vol d'information. Il peut s'agir du vol des numéros de carte de paiement, mais aussi d'informations appartenant à l'un des co-contractants (identifiant et/ou mot de passe, informations personnelles, informations commerciales…).

6.5.3 Chiffrement SSL

Différentes techniques de chiffrement peuvent être envisagées pour assurer la confidentialité de la transaction. Le chiffrement SSL est aujourd'hui la technique la plus répandue.

Le chiffrement SSL consiste à chiffrer les communications entre le serveur web et le navigateur du client au moyen d'une clé privée appartenant au serveur et certifiée par un tiers de confiance.

L'utilisation d'un certificat SSL a un double rôle : il permet de chiffrer les communications, mais aussi d'authentifier les serveurs consultés par le client.

6.5.4 Tiers de paiement

Utiliser les services d'un tiers pour le paiement apporte un certain nombre d'avantages : le commerçant n'a plus la responsabilité du paiement, le client est susceptible d'avoir une confiance plus grande dans un tiers de paiement connu que dans un commerçant inconnu ou moins connu, et les tiers de paiement apportent généralement des infrastructure de non-répudiation.

Enfin, un tiers de paiement est aussi susceptible d'apporter des services complémentaires à la simple sécurité. Ainsi, le problème des micro-paiements (sommes de quelques francs) est plus facile à résoudre en travaillant avec un tiers. Le client pourra par exemple être débité sur sa facture internet, et non sur sa carte bancaire (les paiements par carte bancaire coûtant quelques francs de traitement).

6.5.5 Signature électronique

La signature électronique est un mécanisme permettant d'authentifier les co-signataires d'un document électronique (par exemple, une commande) ainsi que d'assurer l'intégrité du document signé. La législation française a été adaptée au cours de l'année 2000 afin de lui apporter une reconnaissance légale.

Ce mécanisme permet d'apporter une solution au problème de la non-répudiation des échanges. Tout commerçant électronique devrait donc étudier les possibilités d'intégration de la signature électronique afin d'assurer une meilleure sécurité aux échanges avec ses clients.

6.6 Fonctions et données clients

6.6.1 Le contexte

Lors de sa visite, le client échange avec le serveur web de Clusifrance des informations le concernant. Il ne s'agit pas ici des informations échangées dans le protocole http (adresse IP etc.), mais tout simplement de son identité, de son adresse, des produits qu'il commande, de ses moyens de paiement, etc.

Indépendamment de toute velléité de « profilage » de ses clients (technique couramment utilisée pour mettre en place des campagne de marketing « one to one »), Clusifrance a besoin de ces informations pour livrer son client.

Elle possèdent toutefois une très forte valeur marchande, au point que de nombreux sites de commerce électronique considèrent leur base client comme l'un de leurs principaux actifs.

6.6.2 Les menaces : écoute, substitution et piratage.

De par leur grande valeur commerciale, ces informations sont susceptibles d'intéresser un tiers. Celui-ci pourra chercher à les récupérer soit pour ses propres besoins, soit dans le but de nuire au commerçant en annonçant qu'elle ont été récupérées.

La récupération des informations peut s'effectuer d'une par en piratant le serveur dans le but de récupérer directement les fichiers de données (c'est ce qui est le plus souvent pratiqué), d'autre part en interceptant les communications entre le serveur et le client et en les écoutant.

Il est aussi possible qu'un tiers cherche à y opérer des substitutions dans un but quelconque, qui pourra aller d'une attaque contre le serveur (afin de le mettre en déni de service par

exemple) à un acte malveillant envers le client (par exemple, en lui faire acheter une boîte de sardine à 30 000 F !).

6.6.3 Chiffrement SSL – certificat serveur

L'utilisation de chiffrement SSL à l'aide d'un certificat serveur est encore une fois recommandée. Le protocole SSL, en chiffrant les échanges entre le serveur et le client, permet de se prémunir contre les écoutes. Il rend aussi plus difficile les attaques par substitution.

6.6.4 Outils et procédures de lutte anti-pirates

Il est essentiel de gérer la sécurité de son serveur web dans le but d'éviter son piratage. Des outils existent, tels que les firewalls et les systèmes de détection d'intrusion. Toutefois, des procédures de gestion adaptées sont nécessaires.

Une veille des vulnérabilités concernant les logiciels déployés sur le site marchand devra être effectuée, et les correctifs appliqués rapidement. Les mots de passe par défaut des systèmes devront être modifiés : c'est très souvent le moyen utilisé par le pirate pour prendre le contrôle du système.

6.6.5 Chiffrement des fichiers sensibles

Aujourd'hui, il est rare qu'un pirate attaque un site web en écoutant les échanges. Il est généralement plus simple d'attaquer le serveur pour y récupérer des fichiers contenant les informations de dizaines de milliers d'internautes.

Des solutions de chiffrement des fichiers sensibles pourront par conséquent être étudiées : les fichiers récupérés seront alors inutilisables.

6.7 Liaison avec le système de gestion

6.7.1 Le contexte

Le site de Clusifrance a pour but de permettre aux clients de commander des vêtements sur mesure. Cela signifie que chaque vêtement sera fabriqué sur réception des choix du client.

Afin d'obtenir une bonne réactivité et d'éviter les erreurs de transfert, le site a directement été couplé au système de production de l'entreprise, ainsi qu'à ses systèmes comptables, de gestion des stocks, etc.

6.7.2 Les menaces

Bien entendu, ce couplage entraîne des risques pour l'entreprise. Un pirate informatique pourrait tenter de passer par là afin d'obtenir un accès illicite aux systèmes de l'entreprise, ou de les mettre en déni de service.

6.7.3 Mettre en place une architecture adéquate

Il n'y a pas de solution générique correspondant à cette menace. La première mesure à prendre permettant de limiter les risques à ce niveau est de mettre en place une architecture prenant en compte la sécurité du système dès l'origine. Le risques devront être structurellement réduits, afin de pouvoir maîtriser les variables restantes.

6.7.4 Réseaux privés virtuels (VPN)

Une manière d'améliorer la confidentialité des échanges entre le système de gestion et le frontal web marchand est de mettre en place un réseau privé virtuel entre les extrémités du système.

Un réseau privé virtuel (Virtual Private Network, VPN) est ensemble de canaux de communication chiffrés passant sur des réseaux physiques ordinaires. Les échanges transitant par le VPN étant chiffrés, leur interception est difficile, et il est encore plus difficile d'y effectuer des substitutions.

6.8 Mise à jour par l'entreprise

6.8.1 Le contexte

Un site web, marchand ou non, doit être régulièrement mis à jour. Pour les pages HTML, cette mise à jour se fait généralement par le protocole ftp ou par les protocoles de mise à jour des site inclus dans les logiciels de gestion de site. Toutefois, un certain nombre d'informations publiées sur le site peuvent aussi être récupérées automatiquement dans des bases de données. Enfin, de nombreux sites utilisent les services de sociétés tierces spécialisées dans la fourniture d'informations (on parle de techniques de « syndication de contenu ».

6.8.2 Les menaces

Si un tiers arrive à utiliser l'interface de mise à jour du site, il est en mesure d'y faire des modifications profondes. Cet accès privilégié doit donc être particulièrement sécurisé.

6.8.3 Les solutions

La première mesure à mettre en œuvre est l'adoption de procédures de mise à jour clairement définies et soigneusement préparées. Ces procédures devront définir les droits d'accès et les modes de journalisation de ces accès. Des solutions de back-up pourront aussi y être intégrées, afin de pouvoir annuler une modification erronée.

Afin de s'assurer de l'identité de la personne ou du service informatique accédant au site, des outils d'authentification forte pourront être utilisés. Ces outils pourront être par exemple des mots de passe dynamique, l'utilisation de certificats, voire la mise en place de VPN. Les mesures les plus souvent mises en place sont la simple utilisation d'un mot de passe. Si cette procédure peut suffire dans certains cas, il faudra prendre soin que les mots de passe ne circulent pas en clair sur les réseaux.

7 Conclusion : garder une vision d'ensemble

Bénéficiant d'une médiatisation et d'un engouement qui vont de pair avec Internet, le « Commerce Électronique » bouleverse autant nos habitudes de consommateurs que les références et les structures des officines marchandes. Pourtant les références perdurent et bâtir les nouvelles structures de l'e-commerce ne peut s'effectuer que sur des bases solides qui ont fait leurs preuves.

Ainsi, élaborer une solution de commerce électronique doit s'appuyer notamment sur une démarche de sécurité globale et cohérente. Cette démarche est classique :

- Analyser les enjeux. Pour cela il faut identifier les données ayant de l'importance et les classer en fonction de leur valeur et de leur sensibilité.
- Identifier les risques pesant sur l'ensemble du système.
- Mettre en regard les données importantes et les risques pour en déduire les événements que l'architecture de sécurité devra éviter en les classant par ordre de priorité (ex : déni de service, modifications des prix ou des catalogues, vol des fichiers clients...).

La démarche de sécurité doit être structurée et issue d'une réflexion sur les enjeux. Elle ne résulte pas d'une agglomération des derniers produits de sécurité qui font les gros titres de la presse spécialisée.

Les caractéristiques spécifiques d'un site de commerce électronique consistent à prévoir et anticiper la montée en charge de ce site. De plus, l'architecture informatique doit intégrer la souplesse et le renouvellement permanent inhérent au métier du commerce.

Cette approche est simple et classique. Elle a le mérite d'optimiser les coûts, non pas les coûts de la sécurité, mais les coûts de la solution elle-même qui ne peut exister sans sécurité.

En effet, le commerce, qu'il soit traditionnel ou électronique, est toujours basé sur la **confiance**. Cette confiance, qui doit s'établir entre un acheteur et un vendeur, ne s'obtient pas sans sécurité.

8 Glossaire

API	Interface de programme d'application : ensemble de fonctions mises à disposition publique par un programme pour permettre à d'autres programmes de communiquer avec lui.
Applet	(appliquette) Petit programme écrit en langage JAVA, intégré tel quel dans une page HTML.
Autorité de certification	Autorité reconnue pouvant délivrer des certificats.
Java	Langage de programmation développé pour Internet et permettant notamment de faire tourner des applications au sein d'un navigateur (applets).
Browser	Navigateur : logiciel permettant de consulter le web.
BtoB	« Business to business » : relations entre entreprises.
BtoC	« Business to consumer » : relations entre entreprises et consommateurs.
Biclé	Voir Clé privée/publique
Certificats X509	Document électronique émis par une autorité de certification, associant l'identité d'une personne à sa clé publique, garantissant l'authenticité de cette clé publique, et dont la structure est basé sur la norme ISO X509.
CGI (Common Gateway Interface)	Interface de communication entre une application et un serveur Web dans le but de générer des documents dynamiques.
Chiffrement	Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas de clé permettant de le ramener à sa forme initiale. Notes : 1 – Les termes chiffrement et codage ne sont pas équivalents. Alors que le chiffrement fait appel à un algorithme, le codage se fait à partir d'un dictionnaire de codes. 2 – Le terme *cryptage*, attesté aussi bien dans les grands dictionnaires que dans les ouvrages spécialisés où il est employé concurremment avec *chiffrement*, est un dérivé inutile de *cryptographie*. De plus, certains auteurs le donnent comme incorrect. Il ne doit donc pas donner lieu à la création de termes tels que *systèmes de cryptage* (au lieu de *système*

	cryptographique), *cryptage des données* (au lieu de *chiffrement des données*), clé de cryptage (au lieu de *clé de chiffrement*), etc…
	3 – Le terme *chiffrage* fait double emploi avec *chiffrement*, et risque de créer de la confusion puisqu'il désigne aussi l'action d'évaluer en chiffres, par calculs.
	4 – Les termes *encryptage* et *encryption* ne sont attestés par aucun dictionnaire, et sont des synonymes de chiffrement inutiles et risquant d'entraîner la confusion.
	5 – Le terme *brouillage* n'est pas synonyme de chiffrement. Il désigne en effet la perturbation produite sur une ligne de transmission afin de rendre la voix ou les données inintelligibles pour tout le monde.
Clé de chiffrement	Séquence de symboles qui détermine le chiffrement des données, et qui sert également à leur déchiffrement dans un système cryptographique à clé secrète.
Clé secrète ou symétrique	Clé de chiffrement que se partagent l'expéditeur et le destinataire d'un message, le premier pour chiffrer ce message, le second pour le déchiffrer.
Clé privée/publique ou biclé asymétrique	Paire de clés de chiffrement utilisée par les algorithmes asymétriques. La clé publique est accessible à tous les membres d'un réseau ou d'une organisation, et permet de transmettre en toute confidentialité des messages à son unique propriétaire, ou d'authentifier à l'arrivée des messages émis par ce dernier. La clé privée est connue de son unique propriétaire et utilisée par lui seul pour déchiffrer un message dont il est le destinataire, ou pour signer un message dont il est auteur.
Confidentialité (de l'information)	Caractéristique de l'information qui précise son degré de diffusion ou de mise à disposition. Elle exprime aussi le fait qu'elle ne doit pas être connue de tout le monde. Le niveau de confidentialité retenu déterminera le choix des personnes habilitées à en prendre connaissance
CRM (Customer Relationship Management)	Systèmes de suivi de la clientèle très élaborés, intégrant les informations reçues par le Web, non seulement pour la maintenance des produits achetés mais aussi pour développer une vraie politique de fidélisation de la clientèle, ce qui implique autant l'après-vente que le marketing.
C-SET	Voir Set
DdoS (Distributed Denial of Service)	Une attaque en déni de service répartie consiste à générer des flux d'informations adressés à la machine cible depuis un grand nombre de machines relais situées un peu partout sur le réseau Internet
Déni de service	Le déni de service est un type d'attaque informatique qui consiste à rendre un service informatique (par exemple, un serveur Internet) indisponible.
Disponibilité (de l'information)	Caractéristique de l'information prise dans un contexte d'attente de résultat. La disponibilité qualifie l'information "*attendue*" dans sa faculté d'être obtenue avec un temps de réponse satisfaisant, et au moment opportun. Par extension on y associe la notion de pérennité, c'est-à-dire de conservation de cette disponibilité dans le temps.
E-Business	Concept « large »du Commerce Électronique, qui prend en compte les relations de l'entreprise avec ses fournisseurs…

EDI (Electronic Data Interchange)	L'Échange de Données Informatisé est l'échange entre ordinateurs de données concernant des transactions commerciales en utilisant des réseaux et des formats agréés.
FAI	Fournisseur d'accès à Internet (ISP en anglais).
FTP	File Transfer Protocol - Protocole TCP-IP permettant à des ordinateurs d'échanger n'importe quel type de fichiers.
HTTP	Hyper Text Transfer Protocol – Protocole de la suite TCP/IP permettant la navigation dans des pages hyper-texte, reliées par des liens. Ce protocole permet la construction du web.
HTTPS	Combinaison du protocole HTTP utilisant le protocole SSL pour chiffrer les communications.
Hypertexte	Caractéristique de fichiers textes dont certains mots ou groupes de mots sont reliés à d'autres documents par des liens permettant de passer de l'un à l'autre automatiquement
Intégrité (de l'information)	Caractéristique qui qualifie l'information comme étant exempte d'erreur, ou de falsification (acte malveillant). Par extension, on y associe d'autres notions plus ou moins directes, telles que la cohérence, et la complétude.
Intranet	Réseau interne à l'entreprise, utilisant les même outils et protocole qu'Internet.
Internet	Interconnexion de réseaux initialement utilisée par le monde de la recherche et maintenant ouvert à tous, constituant de la sorte un réseau mondial d'information.
ISP (Internet Service Provider)	Fournisseur d'accès à Internet (FAI).
Load-balancing	Répartition de charge entre plusieurs machines.
Mascarade	Menace de l'extérieur liée à l'adressage logique qui se traduit par l'usurpation d'identité consistant à se faire passer pour un utilisateur habilité du système.
OEM	Original Equipment Manufacturer. Revendeur de matériel en assurant lui-même le service après-vente.
Pare-feu (Firewall)	Ensemble de composants (matériels et logiciels) qui bloquent la transmission de certaines classes de trafic
Prévention	Mesure de sécurité dont l'impact agit sur les menaces
Protocole	Séquence de règles à suivre dans les communications pour établir et entretenir des échanges entre des entités distantes.
Rejeu	Message répété intentionnellement en partie ou en totalité. C'est notamment le cas d'un message d'authentification d'échange prélevé et réémis par une autre entité afin de s'en approprier les droits.
Répudiation	Fait pour une personne ou une entité engagée dans une communication de nier avoir participé à tout ou parties des échanges.
Routeur	Machine chargée de gérer le réseau et servant de nœud d'interconnexion
Script CGI	Cf CGI

SET (Secure Electronic Transactions)	Protocole de paiement sur Internet mettant en relation un vendeur, un client et un organisme financier, garantissant la non-répudiation et le recouvrement du paiement, et ne permettant pas au vendeur d'accéder aux moyens de paiement du client.
SMTP	Simple Mail Transfer Protocol : protocole de transmission de la messagerie Internet.
Spamming	Technique de diffusion de messages à caractère commercial à un grand nombre de personnes, sans quelles en aient fait la demande au préalable.
Spoofing	Technique utilisée pour accéder à un ordinateur ou à une information électronique en usurpant l'identité d'un élément autorisé.
SQL	Langage standard d'accès aux bases de données.
SSL	Secure Socket Layers : protocole qui intervient entre le protocole TCP-IP et les différents protocoles applicatifs tels SMTP ou HTTP. SSL est déposé par la société Netscape. Il en existe une version publique standardisée : TLS.
TCP/IP	Suite de protocole de contrôle pour gérer les échanges entre deux machines d'un réseau (sur Internet). IP est le protocole de communication par paquets à la base d'Internet, TCP étant un protocole assurant la validation du transport de paquets. La suite TCP/IP comprend de nombreux autres protocoles (UDP, SMTP, HTTP, FTP…)
Telnet	Protocole d'émulation de terminal permettant d'obtenir à distance une ligne de commande sur un ordinateur. Telnet fait passer « en clair » l'ensemble des échanges, et n'est donc pas sécurisé.
Tiers de confiance	Entité tierce à laquelle des entités communicantes accordent leur confiance pour l'authentification de leurs transactions, et qui peut ainsi certifier l'authenticité des messages émis.
TLS 1.0	Version standardisée publique du protocole SSL v3.0.